Proyecto Fin de Carrera – Ingeniería Informática

Integración de Modelos de Control de Tecnologías de la Información

Autor: Yago Casal Vázquez
Tutor: Juan Miguel Gómez Berbís

Leganés, Mayo de 2014

Tabla de contenidos

Tabla de contenidos 2
1. Introducción 5
1.1. Sistemas de información y Seguridad 6
1.2. Consecuencias de una brecha de seguridad 7
1.2.1. Consecuencias para las compañías 7
1.2.2. Consecuencias para los usuarios 8
1.3. Casos de ejemplo 9
1.3.1. Confidencialidad (Sony Corporation, Abril 2011) 9
1.3.2. Integridad (Stuxnet, Junio 2010) 10
1.3.3. Disponibilidad (Research In Motion, Octubre 2011) 10
2. Estado del arte 12
3. Objetivo 15
3.1. Metodología 16
3.2. Beneficios y limitaciones 21
3.2.1. Beneficios 21
3.2.2. Limitaciones 24
4. Análisis 26
5. Caso de estudio 31
6. Planificación y presupuesto 36
7. Conclusiones 37
8. Líneas futuras 38
9. Agradecimientos 41
10. Anexo I: Referencias 42
10.1. ISO27002 43
10.2. Cobit 44
10.3. ITIL v3 45
10.4. COSO 46
10.5. LOPD 47
10.6. PCI-DSS 49
10.7. SCIIF 50
10.8. SOX 51
11. Anexo II: Detalle a nivel de actividad de control del modelo de control integrado 52

Índice de ilustraciones

Ilustración 1 - Cumplimiento normativo 5
Ilustración 2 - Riesgos TI 6
Ilustración 3 - Modelos de control distribuidos 12
Ilustración 4 - Distribución del cumplimiento 13
Ilustración 5 - Integración modelos de control 15
Ilustración 6 - Modelo de control integrado 16
Ilustración 7 - Metodología 17
Ilustración 8 - Ciclo PDCA 19
Ilustración 9 - Beneficios y limitaciones 21
Ilustración 10 - Beneficios 22
Ilustración 11 - Limitaciones 23
Ilustración 12 - Metodología aplicada 26
Ilustración 13 - Dominios 27
Ilustración 14 - Estructura 27
Ilustración 15 - Grado de cobertura 28
Ilustración 16 - Nivel de cumplimiento 29
Ilustración 17 - Planificación 36
Ilustración 18 - Integración de modelos 37
Ilustración 19 - Futuras líneas 38
Ilustración 20 - Herramientas de auditoría 39
Ilustración 21 - Herramientas de cumplimiento 40
Ilustración 22 - ITIL 45
Ilustración 23 - Ámbitos LOPD 47
Ilustración 24 - Dominios PCI - DSS 49

Índice de tablas

Tabla 1 - Principales regulaciones TI 14
Tabla 2 - Ejemplo de dominio integrado del modelo 57

1. Introducción

Las compañías a día de hoy se encuentran sometidas a una presión normativa y regulatoria cada vez mayor, como regulación en materia de datos de carácter personal (LOPD), en materia financiera (EEFF, SCIIF), etc. Dicha presión normativa y regulatoria es debida a diferentes factores, entre los que cabe destacar los siguientes:

- Legisladores u órganos nacionales e internacionales.
- Necesidades por parte del negocio de cara a obtener certificaciones que avalen la prestación del servicio o la adecuación a normativas sectoriales.
- Procesos o procedimientos internos de la compañía generados por áreas soporte (Seguridad, sistemas de información, etc.).

Tanto las áreas internas de la compañía como los reguladores externos generan nuevos requisitos de cumplimiento normativo:

Ilustración 1 - Cumplimiento normativo

El objetivo primordial de las normativas es la gestión, idealmente a través de la mitigación, de diferentes riesgos, tales como integridad de la información financiera (EEFF, SCIIF), continuidad (ISO22301), confidencialidad de los datos de carácter personal (LOPD) o fraude (Sarbanes Oxley).

La gestión de los riesgos hacia los que se encuentran orientadas las diferentes normativas, estándares, regulaciones, buenas prácticas, etc. a los cuales se ciñen las compañías, repercute en las organizaciones desde diferentes perspectivas: organizativa, técnica, de negocio, así como a seguridad y sistemas de información.

Adicionalmente, el enfoque propuesto generalmente por las normativas para que las entidades aborden la gestión y mitigación de los riesgos que las conciernen es a través de la implementación de modelos de control o governance. Estos modelos de control suelen estar estratificados en procesos, procedimientos o requerimientos.

La conjunción de los modelos de governance provenientes de diferentes normativas, su gestión en todos los niveles de la compañía, junto con su revisión periódica, es lo que

conforma el cumplimiento normativo de una compañía. Por tanto, la tarea principal del cumplimiento normativo es garantizar que, con el menor impacto en el servicio, se evidencie que las compañías han implementado los requerimientos de aquellas legislaciones o normativas de aplicación.

Con el objetivo de gestionar este proceso de cumplimiento normativo se han establecido en muchas entidades departamentos de control interno, auditoría interna o responsables específicos, encargados de desempeñar las funciones de gestión del cumplimiento normativo.

Adicionalmente, la mayor parte de las normativas requieren de un regulador o auditor externo que revise de manera independiente el grado de cumplimiento, para lo cual necesitará que se le evidencie el estado del proceso.

Este factor, unido a las sucesivas revisiones por parte de personal interno y externo provoca que un mismo usuario final tenga que justificar ante diferentes interlocutores el grado de cumplimiento del proceso de cual es responsable repetidas veces.

1.1. Sistemas de información y Seguridad

Los departamentos de sistemas de información y seguridad han ido maximizando la importancia que tienen para los procesos operativos de la compañía, pasando de desempeñar un papel meramente de departamentos soporte a ser parte indispensable en las operaciones de negocio de la compañía.

Asimismo, el impacto mediático del cual gozan los incidentes de seguridad de las entidades hoy en día potencia todavía más la importancia que tienen estos departamentos y genera una reacción normativa por parte de entidades privadas (i.e. PCI-DSS), y públicas a nivel nacional e internacional (i.e. Ley de Infraestructuras críticas, Ley Sarbanes-Oxley).

La tendencia predominante de la regulación en el ámbito de sistemas de información y seguridad va generalmente enfocada a la gestión y mitigación de los siguientes riesgos de la información (de acuerdo a metodologías relativas a la seguridad de la información como Cobit, ITIL, etc.):

- **Confidencialidad**: acceso a la información de la compañía por parte de personas, internas o externas, no autorizadas.

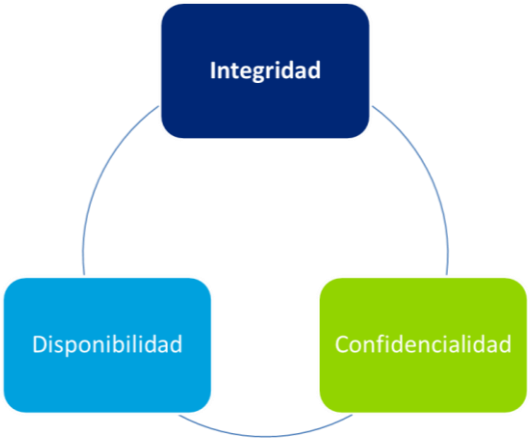

Ilustración 2 - Riesgos TI

- **Integridad**: alteración o corruptibilidad del dato almacenado en los sistemas de información.

- **Disponibilidad**: interrupción en la prestación del servicio por parte de la compañía.

Estos riesgos, presentes en las normativas que afectan al departamento de sistemas e información y seguridad, son gestionados por parte de las normativas a través de una batería de requerimientos, que generalmente impactan en una serie de áreas comunes:

- **Operaciones**: explotación de los sistemas de información, resolución de incidencias, gestión de procesos automáticos, copia de seguridad de los datos, seguridad física de las instalaciones, etc.

- **Seguridad de la información**: sistemas de autenticación de los usuarios, gestión de las altas, bajas y modificaciones de usuarios, trazabilidad de sus acciones, revisiones periódicas, definición de perfiles y segregación de tareas, actualizaciones de seguridad de los sistemas de información, etc.

- **Gestión del cambio**: ciclo de vida de los desarrollos y adquisiciones, segregación de los sistemas por entornos diferenciados y distribución consecuente de los usuarios, ejecución de pruebas técnicas y de usuario de los desarrollos antes de su subida a producción, etc.

Adicionalmente, dentro de las áreas anteriormente mencionadas, las entidades implementan procesos y actividades, muchos de los cuales constituyen requerimientos comunes a un gran número de compañías. Ejemplos de ello pueden ser: la autenticación de los usuarios, las copias de seguridad, la seguridad física de las salas de proceso de datos, etc.

Por tanto, los departamentos de sistemas de información y seguridad extraen la misma información en repetidas ocasiones, para evidenciar su cumplimiento normativo con respecto a diferentes normativas y regulaciones.

1.2. Consecuencias de una brecha de seguridad

En el caso de que los riesgos previamente enumerados se materialicen en una brecha en la seguridad de los sistemas de información, las compañías y los usuarios se enfrentan a un número muy variado de consecuencias.

1.2.1. Consecuencias para las compañías

- **Multas por incumplimiento regulatorio**: un incidente de seguridad puede desencadenar una investigación por las entidades de control de los diversos países en los que se haya producido con el objetivo de verificar si la compañía estaba o no en

cumplimiento con la regulación y, en caso de no estarlo, imponerle las multas relacionadas.

- **Acciones legales de terceros**: las terceras partes afectadas por una brecha de seguridad (como pueden ser los clientes, proveedores o usuarios de una compañía afectada) estarían en disposición de interponer una demanda a la compañía por los daños y perjuicios causados por el incidente. Este tipo de acciones de los usuarios no sólo causan un prejuicio económico sino que comprometen la reputación de la compañía.

- **Daños colaterales**: el restablecimiento de la situación inicial, la situación previa al incidente, puede tener un gran coste indirecto, a consecuencia de demandas, acuerdos, pérdidas de clientes así como restitución de credenciales (usuarios, contraseñas, tarjetas de crédito, etc.). Adicionalmente, en caso de comprometer los sistemas de información, la recuperación de la operatividad de los mismos, en caso de que la entidad disponga de un plan de continuidad, suele conllevar un esfuerzo económico de importancia.

- **Valor de la compañía**: habitualmente, de forma posterior al sufrimiento de un ataque llevado a cabo de forma satisfactoria, el valor de la compañía en bolsa desciende notablemente en puntos porcentuales.

- **Reputación corporativa**: el nivel de seguridad que una compañía transmite a la opinión pública se ve gravemente resentida cuando un atacante consigue acceder a los sistemas de la misma. La sensación de vulnerabilidad ofrecida es duradera y la restitución de la confianza del público es una tarea ardua.

- **Venta de información**: en caso de que la información comprometida sea, de alguna forma, estratégica para la compañía; dichos datos podrían ser vendidos o filtrados a la competencia, resultando en futuras pérdidas.

1.2.2. Consecuencias para los usuarios

- **Ataques de suplantación de identidad o *Phishing***: mediante los datos obtenidos en el incidente, los atacantes podrían utilizar la información a la que han accedido para realizar ataques de ingeniería social, a través de los cuales se pretende adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

- **Robo de identidad**: si los datos obtenidos son suficientes (o completados mediante un ataque de *Phishing*), el atacante podría suplantar al usuario afectado a la hora de realizar transacciones electrónicas, económicas, sanitarias, etc.

- **Acceso a servicios de terceros**: de manera muy común, los usuarios emplean la misma contraseña para acceder a los diversos servicios on-line que emplean. Es por ello que la obtención de la contraseña utilizada por el usuario en el servicio afectado podría permitir su uso en muchos otros.

- **Uso de los datos sin consentimiento**: la información de los usuarios obtenida de manera fraudulenta puede ser utilizada para realizar acciones de marketing o promoción, sin el consentimiento explícito del usuario.

1.3. Casos de ejemplo

Como muestra de la importancia que ha adquirido la seguridad de los sistemas y, por tanto, la normativa vigente que regula la aplicación de diferentes medidas de cara a asegurar la no vulnerabilidad de los mismos, se detallan ejemplos recientes de diversas brechas de seguridad asociadas a los principales riesgos descritos anteriormente así como las consecuencias derivadas de las mismas para las compañías afectadas.

1.3.1. Confidencialidad (Sony Corporation, Abril 2011)

Entre los días 17 y 19 de Abril de 2011, Sony Corporation sufrió una intrusión de alcance masivo en su red, que permitió desvelar los datos personales y bancarios de los usuarios de *PlayStation Network* (plataforma desarrollada para la venta de contenidos digitales y el soporte del juego en línea accesible mediante diversos sistemas de entretenimiento digital) y *Qriocity* (actualmente conocido como *Music Unlimited*, servicio de música *streaming* bajo demanda).

Fruto de ello, el atacante tuvo acceso a los datos personales como nombre, dirección, cuenta de correo electrónico o fecha de nacimiento de **77 millones de usuarios en 59 países**, conociendo también sus nombres de usuario y contraseñas, según informó la empresa. En dicha fecha en España existían 3.000.000 de cuentas de *PlayStation Network*, de las cuales 330.000 incluían información acerca de tarjetas de crédito.

Adicionalmente, y como medida de prevención, la plataforma *PlayStation Network* se mantuvo inactiva más de dos semanas.

A consecuencia de dicho ataque, el prestigioso instituto de investigación Ponemon (fundado en 2002 y con sede en Michigan) estimó que la violación de su base datos puede suponerle a Sony un coste superior a **1.500 millones de dólares** (1.010 millones de euros).

Este suceso provocó las investigaciones y denuncias de diversas organizaciones y agencias como fueron la Agencia Española de Protección de Datos (AEPD) en España, el *Information Commissioner's Office* (ICO) en Reino Unido y numerosos bufetes de abogados defensores de los consumidores en Estados Unidos.

Por último, la situación supuso una ventaja a su más directo competidor en el área de entretenimiento on-line, provocando la atracción de una notable cantidad de usuarios a sus servicios; por considerarlos más fiables.

1.3.2. Integridad (Stuxnet, Junio 2010)

En junio de 2010, la compañía de seguridad bielorrusa VirusBlokAda descubrió un gusano informático que alteró el funcionamiento de un proceso industrial, ya que fue diseñado con la finalidad de dañar equipos físicos y modificar las indicaciones de los operadores a cargo de la supervisión, para impedir, de este modo, que se identificara cualquier anomalía en los equipos.

Dicho gusano infectó la central nuclear Natanz, en Irán. La central iraní usaba centrifugadoras para enriquecer uranio.

Los creadores de Stuxnet podrían haber destrozado totalmente las instalaciones nucleares de Natanz. Sin embargo, aunque no lo hicieron, aun así consiguieron sus propósitos: retrasar el programa nuclear iraní.

El ataque del gusano tuvo como objetivo una central nuclear, una infraestructura altamente protegida.

Si esta modalidad de ataque a la integridad de los datos (denominado también “ataque semántico”) se hubiera replicado en otros sistemas, podría haber causado problemas graves en infraestructuras informáticas de importancia crítica, como las de servicios públicos, servicios de urgencia, control de tráfico aéreo y cualquier otro sistema que dependa en gran medida de las tecnologías de la información y resulte indispensable para la sociedad. Este tipo de infraestructuras también son mucho más vulnerables por la estandarización: es mucho más fácil conseguir los diseños y encontrar fallos de los sistemas en ellas que en centrales nucleares.

1.3.3. Disponibilidad (Research In Motion, Octubre 2011)

En el mes de octubre de 2011, más concretamente entre los días 11 y 14, el servicio de internet BlackBerry (servicio de sincronización y correo electrónico proporcionado por Research In Motion [RIM] para los usuarios de dispositivos BlackBerry) mantuvo una avería continua que provocó la caída de todo el sistema y dejó a decenas de millones de usuarios de este dispositivo móvil en los cincos continentes sin correo electrónico, mensajería instantánea y navegación. Durante el fallo, los clientes sólo pudieron hablar por teléfono y mandar SMS desde sus dispositivos, pero no acceder a cualquier servicio basado en la red.

RIM utiliza sus propios servidores para enviar y recibir mensajes, tanto de correo electrónico como de texto, en todo el mundo, lo que hace que el sistema sea vulnerable a caídas en cascada.

Su independencia es uno de los principales atractivos para muchos usuarios en diversas regiones del mundo, dado que sus comunicaciones no pueden ser interceptadas por las autoridades locales.

Según la explicación de la compañía, cuando falló uno de sus servidores centrales, uno de los *switches* del núcleo de su red, que teóricamente estaban configurados para trabajar en alta disponibilidad y debía redirigir el tráfico al resto de la infraestructura en caso de fallo, no realizó tal función y, por tanto, los usuarios se quedaron sin servicio. Cuando RIM intentó solventar el problema, el tráfico acumulado pendiente de cursar era de tal magnitud que, al aplicar el balanceo sobre el resto de servidores, éstos se colapsaron y llegaron a un punto de congestión que se extendió más allá del territorio Europa, Oriente Medio y África (EMEA, por sus siglas en inglés), que fue el que sufrió el fallo el primer día.

Se calcula que RIM ganaba al menos 3’4 millones de dólares (2’4 millones de euros) por día en los ingresos por el servicio.

2. Estado del arte

Las normativas, regulaciones o buenas prácticas proponen generalmente la implementación de sus requerimientos a través de modelos de control, que deben ser establecidos por las compañías en su operativa:

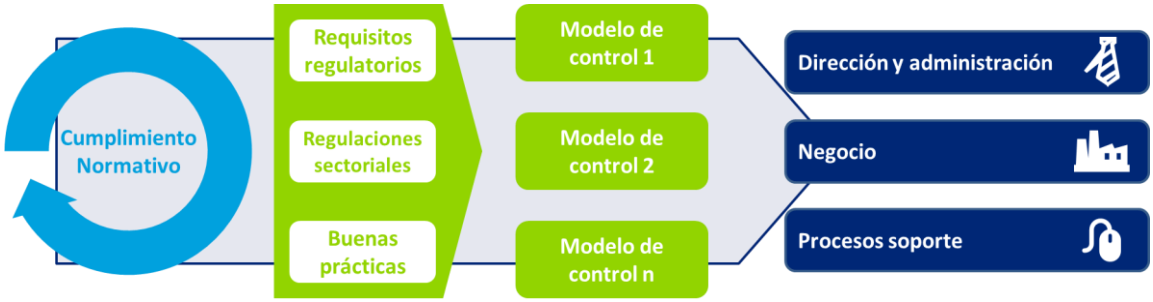

Ilustración 3 - Modelos de control distribuidos

Los requerimientos de los modelos de control de normativas o buenas prácticas presentan un enfoque basado en los siguientes aspectos:

- **Formalización de los procesos y operaciones**, principalmente con los objetivos de establecer una guía homogénea para la ejecución de los mismos, evitar pérdida de conocimiento o dependencias de personal, así como facilitar la inspección por parte de un tercero.

- **Trazabilidad de eventos:** generación de un registro o soporte que contenga la información suficiente de los mismos para que pueda ser objeto de auditoría o revisión.

- **Baterías de controles**, implementación y operación de controles de manera periódica y manteniendo evidencia de ello.

- **Responsabilidad de las tareas**, evitando la alegación del desconocimiento por parte de los actores y personal involucrado.

Por tanto, un modelo de control que afecte a un área de una entidad conlleva un esfuerzo por parte del área a la hora de documentar sus procesos, almacenar evidencias y ejecutar controles. Conlleva también otro esfuerzo inherente, que consiste en demostrar periódicamente su grado de cumplimiento, revisado periódicamente tanto por personal interno como por parte de personal externo.

Dentro del ámbito ya de sistemas de información y seguridad, existe un gran número de normativas y regulaciones con impacto, por lo que existe una cantidad notable de modelos de control destinados a dar cobertura a sus correspondientes requerimientos. En el ámbito de sistemas de información y seguridad, existe un porcentaje significativo de los requerimientos que componen los modelos de control de diferentes normativas que son comunes.

La principal característica del cumplimiento normativo en el área de sistemas de información y seguridad en una gran variedad de entidades y sectores, tales como telecomunicaciones, energía o productos y servicios, es que **el cumplimiento normativo se aborda de manera reactiva**. Ello implica que generalmente los requerimientos normativos son abordados como consecuencia de la revisión de cumplimiento y que aquellos sistemas de información que no se hallan en el alcance de ninguna normativa no disponen de una mitigación de riesgos de TI suficiente.

Otros aspectos a destacar en relación a la actividad de cumplimiento normativo de las entidades son:

- La **no formalización de un modelo de control** a excepción de que sea explícitamente requerido por la normativa o regulación (por ejemplo, Sarbanes-Oxley o SCIIF). El motivo de ello fue la reducción de esfuerzo por parte de las entidades, si bien al contar con una combinatoria de normativas sin modelo de control formalizado, el proceso de cumplimiento se vuelve más complejo.

  Asimismo, la no formalización de un modelo de control dificulta la tarea de los ejecutores o administradores de las actividades de control, al no existir formalización de las responsabilidades, planificación, pérdida del conocimiento adquirido, etc.

- El proceso de **cumplimiento normativo se encuentra distribuido** y desagregado a lo largo de la organización, ejecutándose de diferentes enfoques. Esto es consecuencia de que las diferentes áreas de la entidad fueron abanderando el cumplimiento las regulaciones o normativas que impactaban directamente en su actividad:

Ilustración 4 - Distribución del cumplimiento

Existen entidades en las cuales sí existe una centralización a través de una figura que aglutina total o parcialmente el proceso de cumplimiento normativo. Asimismo, esta figura sí dispone de los conocimientos necesarios para identificar las sinergias existentes entre requerimientos normativos e integrar las actividades de control, si bien, aun cuando este conocimiento se aplica en la operativa diaria, no se encuentra formalizado.

- Falta de concienciación en la organización en relación al cumplimiento normativo en el área de sistemas de información y seguridad. Consecuencia de los aspectos anteriores, que conllevan una falta de planificación y poca formalización, es que los operadores y ejecutores de las actividades de control son requeridos a obtener la misma información repetidas veces, por diferentes actores internos y externos y sin ser conscientes del motivo por el cual la información está siendo requerida.

Se incluye a continuación un breve resumen de las principales normativas, regulaciones y buenas prácticas con impacto en los sistemas de información que conforman el cumplimiento normativo de las compañías y que han sido mencionadas en el presente documento (consultar el Anexo I: Referencias para mayor detalle):

Normativa / regulación	Acrónimo	Tipología	Objetivo	Alcance	Implicaciones en Sistemas de Información
Estados Financieros	EEFF	Regulatorio	Garantizar la fidelidad de las cuentas de la compañía	Cualquier evento en el ámbito de la entidad con impacto en los estados financieros	Realización de un conjunto de procedimientos de cara a garantizar la integridad, confidencialidad y disponibilidad de aquellos sistemas de información que traten datos con impacto en los estados financieros de la entidad
Ley orgánica de protección de datos	LOPD	Regulatorio	Confidencialidad de datos de carácter personal	Aquellos tratamientos de datos de carácter personal de la entidad	Implementación de un conjunto de medidas organizativas, técnicas y legales
Sarbanes Oxley	SOX	Regulatorio	Evitar que los directivos de la compañía manifiesten desconocimiento ante la situación financiera de una entidad	Procesos de la entidad con impacto significativo en los estados financieros	Implementación de un modelo de control a ser revisado tanto internamente como por un tercero
ISO27001	ISO27001	Buenas prácticas	Establecer un marco para la gestión de la seguridad de la información	A definir por la entidad	Implementación de un conjunto de actividades de control y de un proceso de mejora continua de dicho conjunto
Sistema de Control de la Información Financiera	SCIIF	Buenas prácticas	Garantizar la fidelidad de las cuentas de la compañía	Procesos de la entidad con impacto significativo en los estados financieros	Implementación de un modelo de control interno sobre aquellos procesos con impacto en los estados financieros

Tabla 1 - Principales regulaciones TI

3. Objetivo

El objetivo perseguido en el proyecto es formalizar un **modelo de control integrado** en el ámbito de sistemas de información y seguridad, a través de la identificación e integración de sinergias en los requerimientos normativos, con el objetivo de consolidar y optimizar el cumplimiento regulatorio.

Por tanto, el proceso de cumplimiento normativo, realizado de manera reactiva mediante modelos de control distribuidos, debe ser modificado:

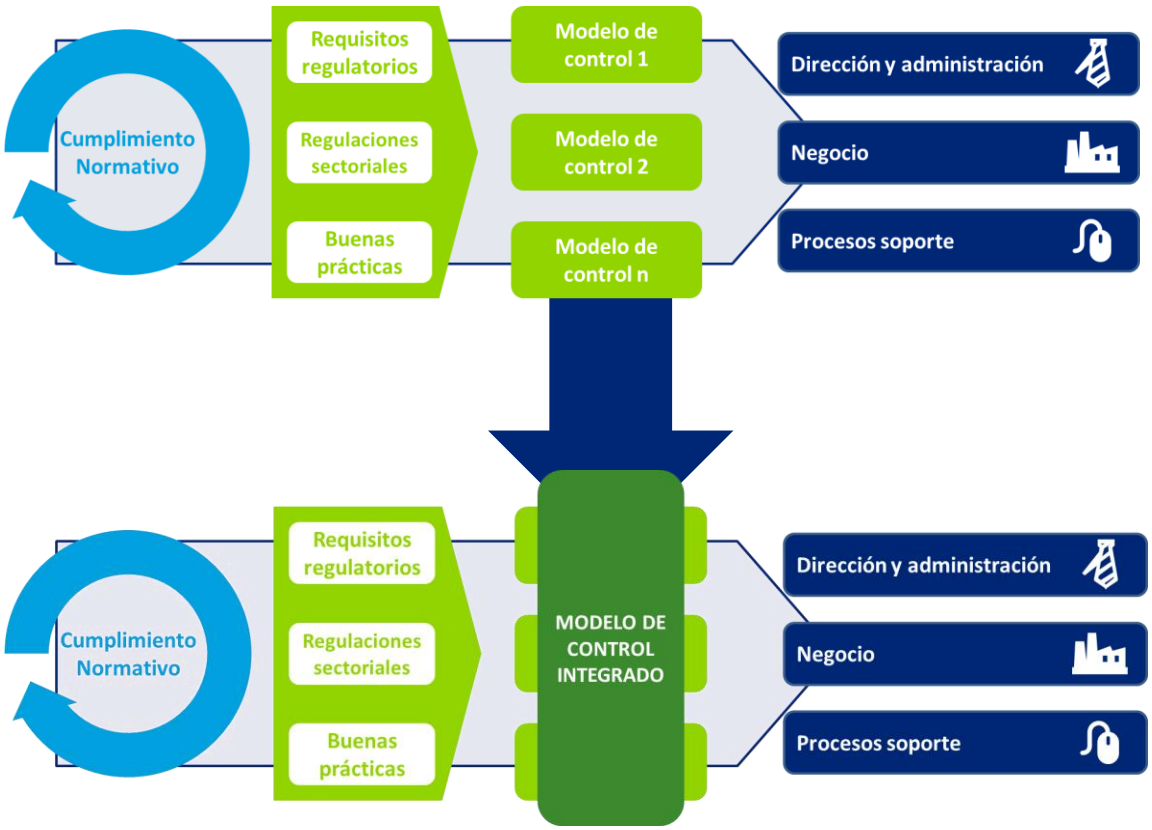

Ilustración 5 - Integración modelos de control

El modelo de control integrado debe dar cumplimiento a los requerimientos regulatorios de las normativas aplicables con la suficiente profundidad. Asimismo, debe ser completo a fin de mitigar los principales riesgos relativos a los sistemas de información.

El modelo de control integrado que se ha definido en el presente documento da cobertura a los requerimientos de las siguientes normativas o buenas prácticas:

- ISO27002.
- Cobit.
- ITIL v3.
- COSO.
- PCI-DSS.
- SCIIF.

- SOX.

Se han seleccionado las normativas anteriores por constituir las más habituales o requeridas por las compañías en su proceso de cumplimiento normativo.

Asimismo, con el objetivo de que el modelo de control presente cobertura frente a los principales riesgos TI, se han considerado un conjunto de actividades de control adicionales, catalogadas como Normativa Interna.

El ejercicio realizado es teórico, focalizado en la definición del modelo de control de la entidad en lugar de en las tareas relativas a la implantación y revisión del modelo de control. Las tareas concretas de la metodología seguida que han sido asumidas se detallan en el apartado 4 Análisis.

Ilustración 6 - Modelo de control integrado

3.1. Metodología

La formalización del modelo de control integrado se ha realizado siguiendo la metodología detallada a continuación:

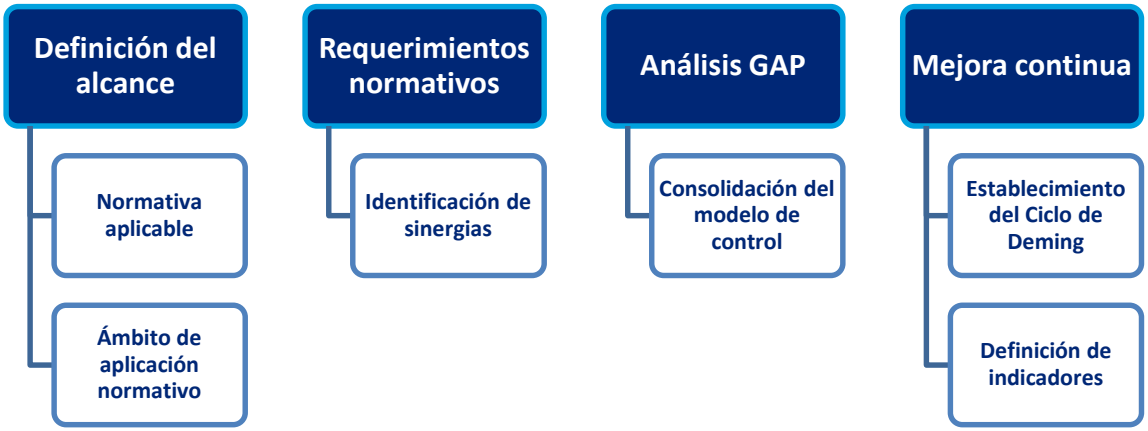

Ilustración 7 - Metodología

Las fases e hitos que componen la metodología propuesta para la definición, implantación y mantenimiento del modelo de control integrado, se establecen a continuación:

Definición del alcance

- Normativa aplicable: se ha de determinar las normativas a incorporar al marco de control integrado, teniendo en cuenta las necesidades de las diferentes áreas de la compañía, que han sido divididas en:

  - Requerimientos regulatorios: constituyen aquellos de obligado cumplimiento debido al dictamen de organismos nacionales o internacionales.

  - Regulaciones sectoriales: aquellas normativas inherentes a la actividad desarrollada por la entidad.

  - Buenas prácticas: estándares propuestos a los cuales la compañía se quiere adecuar o certificar.

  Asimismo, debido a que el modelo de control integrado simplifica la adecuación de la entidad a nuevas normativas, adicionalmente se deben considerar aquellos estándares o regulaciones a los que la entidad considere necesario adecuarse próximamente.

  El output de esta tarea es el listado de regulaciones, normativas y buenas prácticas que forman parte del cumplimiento normativo de la compañía.

- Ámbito de aplicación normativo: la tipología de información sobre la cual se focalizan las normativas o estándares difiere. Por ejemplo, el Sistema de Control Interno de la Información Financiera (SCIIF) o la Ley Sarbanes-Oxley (SOX) se focalizan en la información financiera, y ésta última más concretamente en el riesgo de fraude al que está expuesto la información financiera. Por el contrario, la Ley Orgánica de Protección de Datos (LOPD), a través de su Reglamento de Desarrollo (RDLOPD), se centra en los datos de carácter personal que trata la compañía. Finalmente, en el caso de la ISO 27001, el ámbito de aplicación no es establecido

por la normativa, sino que es decisión de la entidad qué procesos o servicios estarán incluidos en su ámbito.

En el área de sistemas de información, los requerimientos de las diferentes normativas serán de aplicación sobre conjuntos de sistemas de información diferenciados. El alcance del modelo de control integrado estará compuesto fundamentalmente por aquellos sistemas que figuran como de aplicación para diferentes normativas.

A consecuencia de esta fase, se ha definido el alcance del modelo de control integrado, compuesto por las normativas, regulaciones o estándares que engloba, así como los sistemas de información a los que impacta cada una.

Requerimientos normativos

- Identificación de sinergias: el modelo de control integrado debe dar cumplimiento a todos los requerimientos de las regulaciones definidas en el alcance, si bien se deben identificar y combinar los requerimientos comunes en actividades de control únicas.

  Asimismo, con el objetivo de garantizar que el modelo de control integrado proporciona cobertura a los principales riesgos en el ámbito de los sistemas de información y seguridad, se deberá analizar la necesidad de completar el modelo de control integrado con actividades de control adicionales.

El resultante de esta fase está conformado por un conjunto de actividades de control específicas que compondrán el modelo de control integrado, identificando las normativas que están siendo cubiertas por cada actividad.

Análisis del grado de madurez (GAP)

- Consolidación del modelo de control: habiendo definido y unificado un conjunto de actividades de control que proporcionan cobertura frente a los diferentes requerimientos normativos y regulatorios, se debe realizar un análisis para verificar el grado de implantación del modelo en la operativa diaria de la entidad.

  El análisis del grado de implantación del modelo se realizará a través de un programa de auditorías en base a los cuales se podrá determinar el grado de implantación de las actividades de control definidas en el modelo en la operativa de una entidad.

Mediante esta fase, la entidad podrá determinar el nivel de consolidación del modelo de control definido en la operativa diaria.

Mejora continua

- Establecimiento del Ciclo de Deming de Mejora Continua: el entorno normativo con

el cual conviven las entidades es cambiante, por lo que se debe establecer un proceso de mejora continua, con el objeto de que el modelo de control no se vuelva obsoleto.

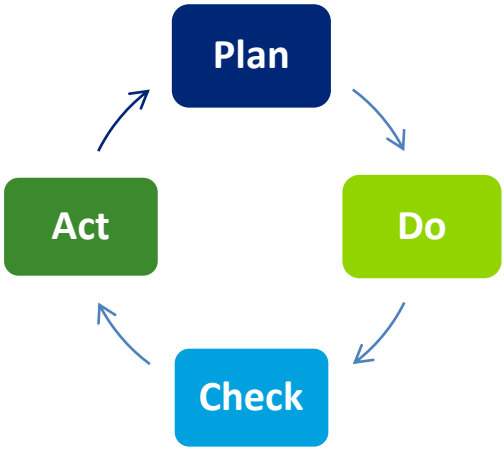

Ilustración 8 - Ciclo PDCA

El ciclo de Deming establece cuatro fases que deben ser ejecutadas reiterativamente, si bien las tres primeras fases Plan, Do y Check han sido ejecutadas ya una vez como parte de la presente metodología.

El período en el cual el Ciclo de Deming debe ser ejecutado iterativamente sobre el modelo de control integrado es generalmente coincidente con el año fiscal de la entidad.

La fase que no ha sido ejecutada en los pasos anteriores es Act. A consecuencia del programa de auditorías se obtendrán un conjunto de puntos de mejora o acciones a implementar, los cuales se deberán incorporar a un plan de acción del que se deberá realizar un seguimiento en esta fase y en las iteraciones siguientes del Ciclo.

La reiterativa ejecución de las fases del Ciclo de Deming en el modelo de control integrado debería estar constituida por:

- Plan: el alcance del modelo de control debe ser objeto de revisión, adecuando el listado de normativas en alcance y adecuando consecuentemente los sistemas de información que serán cubiertos.

  Las normativas que conforman del modelo de control integrado no deberían sufrir variaciones significativas, a excepción de normativas puntuales que sean incorporadas.

  El listado de aplicaciones sí es probable que se vea alterado, de manera consecuente con el punto anterior, o bien a través de migraciones de sistemas, integraciones o por la propia evolución del negocio. Por ejemplo, la disminución de impacto económico de una línea de negocio sobre los estados financieros de la compañía provocará que ciertos sistemas no estén en el alcance de ciertas normativas.

- Do: a consecuencia de la incorporación de nuevas normativas al modelo de control, se deberán integrar sus requerimientos en las actividades de control

definidas, o bien definir actividades de control adicionales que soporten los requerimientos no cubiertos.

Asimismo, en el caso de incorporar nuevos sistemas de información al alcance del modelo, se deberá analizar si dichos sistemas se adecúan a las actividades de control aplicables definidas en el modelo.

- Check: el programa de auditorías al cual esté sujeta la entidad permitirá determinar su grado de cumplimiento normativo y proporcionar la entrada para la definición de los planes de acción y mejora correspondientes.

- Act: las acciones contenidas en los planes de acción definidos a consecuencia del programa de auditorías deberán ser analizadas desde un punto de vista de viabilidad, y planificada su implementación si procede.

El resultado obtenido tras la ejecución de este hito es la definición, planificación e implementación de un plan de acciones correctoras, a consecuencia del análisis GAP realizado anteriormente.

- Definición de indicadores: el ciclo PDCA requiere el establecimiento de un conjunto de indicadores en base a los cuales se permita el gobierno del modelo de control. En el contexto del modelo de control integrado, las tipologías de indicadores que aportan mayor visibilidad sobre el modelo de control integrado son:

  - Por normativa: indicadores acerca del cumplimiento normativo existente en la entidad para una normativa concreta. Por ejemplo, actividades de control definidas, grado de cumplimiento con las actividades de control en diseño, implementación o eficacia operativa, etc.

  - Por sistema: indicadores relativos al cumplimiento de un sistema de información con respecto a las normativas o regulaciones aplicables. Por ejemplo, actividades de control definidas por sistema, acciones correctoras establecidas en los planes de acción, etc.

  - Por dominio: las actividades del modelo de control integrado se agrupan generalmente en dominios, objetivos de control o áreas. La operativa contenida en dichos dominios suele ser ejecutada por la misma unidad organizativa o dirección. Ejemplos de indicadores por dominio podrían ser: número de actividades de control correctamente implementadas, planes de acción en curso, etc.

  - Por tecnología: existen dominios concretos en los cuales la implementación de las actividades de control varía significativamente en función de la tecnología, como por ejemplo la autenticación y autorización en los sistemas de información. Asimismo, suelen ser unidades organizativas diferenciadas quienes implementan dichas actividades de control.

La consecuencia de este hito será el establecimiento de un cuadro de mandos del modelo de control integrado.

El resultante de esta fase de la metodología será la definición de un plan de acciones correctoras, así como un cuadro de mandos que permita el gobierno del modelo de control integrado.

3.2. Beneficios y limitaciones

El modelo de control integrado aporta un conjunto de beneficios a diferentes procesos de la entidad, destacando el proceso de cumplimiento normativo, y presenta también un conjunto de limitaciones:

3.2.1. Beneficios

Los beneficios que proporciona el modelo de control integrado han sido estructurados en dos bloques, cumplimiento normativo y organización, que a su vez se han desagregado en dos vertientes cada uno:

Ilustración 9 - Beneficios y limitaciones

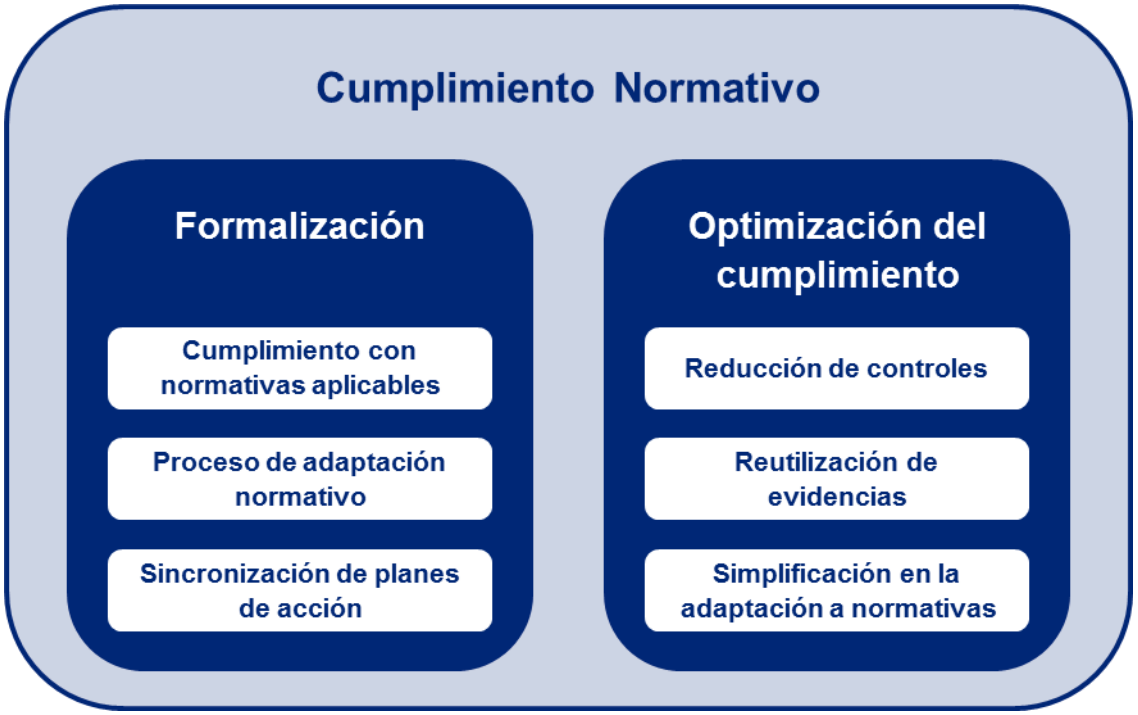

Ilustración 10 - Beneficios

El proceso de cumplimiento normativo se ve sustancialmente impactado por el modelo de control integrado, principalmente en dos vertientes:

- **Formalización**

    - **Cumplimiento con normativas aplicables:** el grado de cumplimiento de una entidad con las normativas aplicables mejora a consecuencia de la definición e implementación de un modelo de control integrado, por ejemplo, gracias a: la unificación de las actividades de control existentes en la entidad, establecimiento de responsabilidades a través de la organización, la formalización de un calendario de cumplimiento, etc.

    - **Proceso de adaptación normativo:** el proceso a seguir por parte de una entidad para adecuarse a una nueva normativa o regulación queda definido, ya que constituye una de las actividades que conforman la metodología de diseño e implementación del modelo de control integrado.

    - **Sincronización de planes de acción:** el modelo de control integrado permite establecer un plan de acciones correctoras unificado y coherente, a raíz de las diferentes auditorías requeridas por cada normativa, que simplifique la planificación e implementación de las mismas.

- **Optimización del cumplimiento**

- **Reducción de controles:** el volumen de controles con los que la compañía debe cumplir se ve reducido gracias a la identificación de sinergias en los requerimientos normativos.

- **Reutilización de evidencias:** una consecuencia directa de la unificación de requerimientos normativos es la reutilización de evidencias, evitando que estas tengan que ser extraídas por la entidad en sucesivas ocasiones.

- **Simplificación en la adaptación a normativas:** el proceso de adecuación a nuevas normativas por parte de la compañía se formaliza y se simplifica, ya que se reduce a la contraposición de los requerimientos normativos al modelo de control integrado.

Ilustración 11 - Limitaciones

Desde un punto de vista organizacional, el modelo de control integrado proporciona también un conjunto de beneficios, que han sido agrupados en dos bloques:

- **Reporte**:

  - **Visibilidad:** la definición e implementación de un modelo de control integrado proporciona mayor visibilidad al cumplimiento normativo dentro de la entidad.

- **Cuadros de mando:** el establecimiento de un conjunto de indicadores de cumplimiento normativo, agrupados en un cuadro de mando, permiten el reporte a la dirección del estado del modelo de control integrado y simplifican su percepción y contextualización en la organización.

- **Monitorización continuada**: el modelo de control integrado permite disponer, a través de sus indicadores, de una monitorización continuada de su grado de cumplimiento, así como del grado de avance de los planes de acción definidos, etc.

- **Gobierno**:

  - **Centralización de alcances**: la gestión y mantenimiento de los alcances a los que afectan las diferentes normativas se centraliza y unifica, evitando la existencia de desactualizaciones o duplicidades.

  - **Ejecución de actividades de control**: la ejecución de actividades de control por parte de sus correspondientes responsables o administradores se formaliza, gracias al establecimiento de un responsable definido, fechas de reporte, unificación de acciones correctoras, etc.

  - **Planificación de auditorías**: la definición del alcance del modelo de control integrado, conformado por las normativas aplicables y por los sistemas de información afectados, permite planificar las auditorías que se van a ejecutar a lo largo del período, optimizando los tiempos de respuesta de la compañía al cumplimiento normativo.

3.2.2.Limitaciones

El modelo de control integrado presenta también un conjunto de limitaciones en la actividad de cumplimiento normativo, que se destacan a continuación:

- La definición del modelo de control integrado no implica una reducción del cumplimiento normativo:

  - El número de auditorías a los que estará sometida la entidad no variará, puesto que el listado de normativas y regulaciones a los que la entidad está sujeta sigue siendo el mismo.

  - Los diferentes auditores obtienen conclusiones independientes acerca del grado de cumplimiento de la entidad, a pesar de que se posibilite la reutilización de evidencias en aquellas actividades de control comunes.

- La metodología en base a la cual se auditan las diferentes normativas puede variar, por lo que resulta complicado que algunos auditores basen sus resultados en el trabajo de otros. Por ejemplo, un auditor del RDLOPD analizará los requerimientos correspondientes desde un punto de vista de diseño e implementación, mientras que un auditor SCIIF analizará la formalización de las actividades de control correspondientes, así como el diseño, la implementación y la eficacia operativa de las mismas. Por ello, si bien el auditor SCIIF podría basar parte de su trabajo en lo realizado por el auditor del RDLOPD, ello no sería suficiente para la emisión de sus conclusiones.

- La identificación de requerimientos comunes en una actividad de control única es siempre posible desde una perspectiva de diseño de la actividad de control, si bien puede no serlo en el caso de la implementación.

4. Análisis

El trabajo realizado para la definición del modelo de control TI es el siguiente, de acuerdo a la metodología definida:

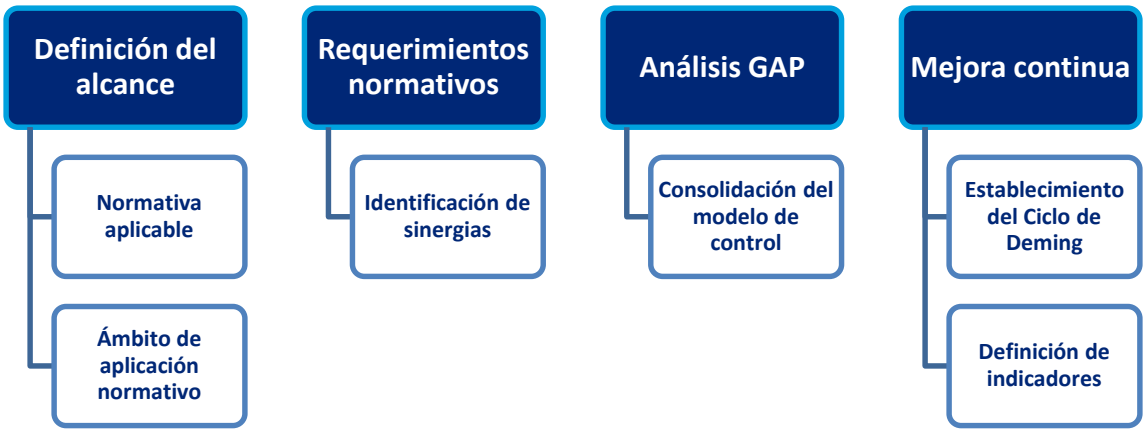

Ilustración 12 - Metodología aplicada

Definición del alcance

- Normativa aplicable: se han elegido un conjunto de normativas, regulaciones y buenas prácticas sobre las cuales se realizará la integración de sus modelos de control:

  - ISO27002.
  - Cobit.
  - ITIL v3.
  - COSO.
  - PCI-DSS.
  - SCIIF.
  - SOX.

  Tal y como se ha indicado previamente, se han seleccionado las normativas, regulaciones y buenas prácticas por constituir las más habituales en el proceso de cumplimiento normativo de las entidades o bien por ser las más demandadas en el ámbito de los sistemas de información.

- Ámbito de aplicación normativo: el listado de aplicaciones sobre las que impactan cada una de las normativas no se ha podido establecer ya que depende del entorno de sistemas de información de una entidad, si bien ello no repercute en la definición de las actividades de control.

Requerimientos normativos

- Identificación de sinergias: los requerimientos normativos del alcance seleccionado han sido analizados con el objetivo de identificar y formalizar las sinergias

existentes.

En base a ello, se ha definido una batería de controles, dividida en 9 dominios, estructurados en subdominios y a su vez compuestos por actividades de control, para cada una de las cuales se han indicado los apartados, secciones o artículos correspondientes de las normativas que se encuentran cubiertos:

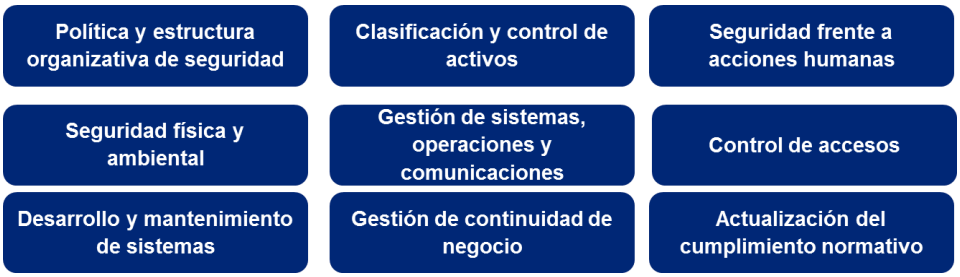

Ilustración 13 - Dominios

La estructura conformada por los dominios, subdominios y actividades de control del modelo de control integrado se encuentra detallada a continuación.

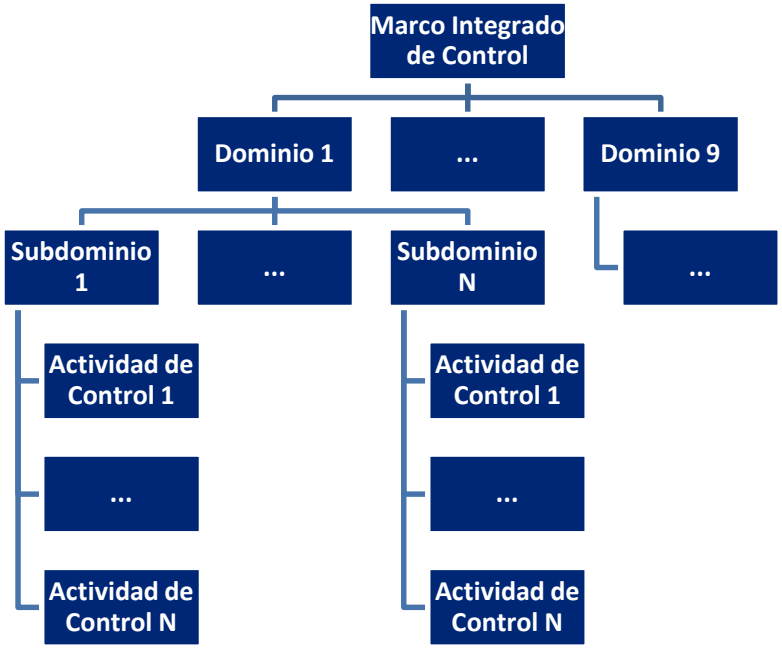

Ilustración 14 - Estructura

Adicionalmente, se incluye en el Anexo II un ejemplo detallado de la integración llevada a cabo a nivel de actividad de control para un subdominio. Se indica, para cada una de las actividades de control en alcance los apartados, secciones o artículos correspondientes de las normativas que se encuentran cubiertos.

Análisis GAP

- Consolidación del modelo de control: el análisis de la situación de una entidad con respecto al modelo de control no ha sido efectuada, puesto que sería necesario

realizar una auditoría del modelo de control en el entorno de sistemas de información de una entidad.

Mejora continua

- Establecimiento del Ciclo de Deming: el plan de acción, a consecuencia del Análisis GAP no se ha definido.
- Definición de indicadores: se dividen en dos tipologías:
  - Diagrama del grado de cobertura normativa: número de normativas con las que se mapea cada actividad de control.

    A modo de ejemplo se detalla a continuación el diagrama de nivel de alcance de un dominio en particular, es decir, el número de requerimientos normativos que están siendo cubiertos por las actividades de control definidas en el modelo integrado:

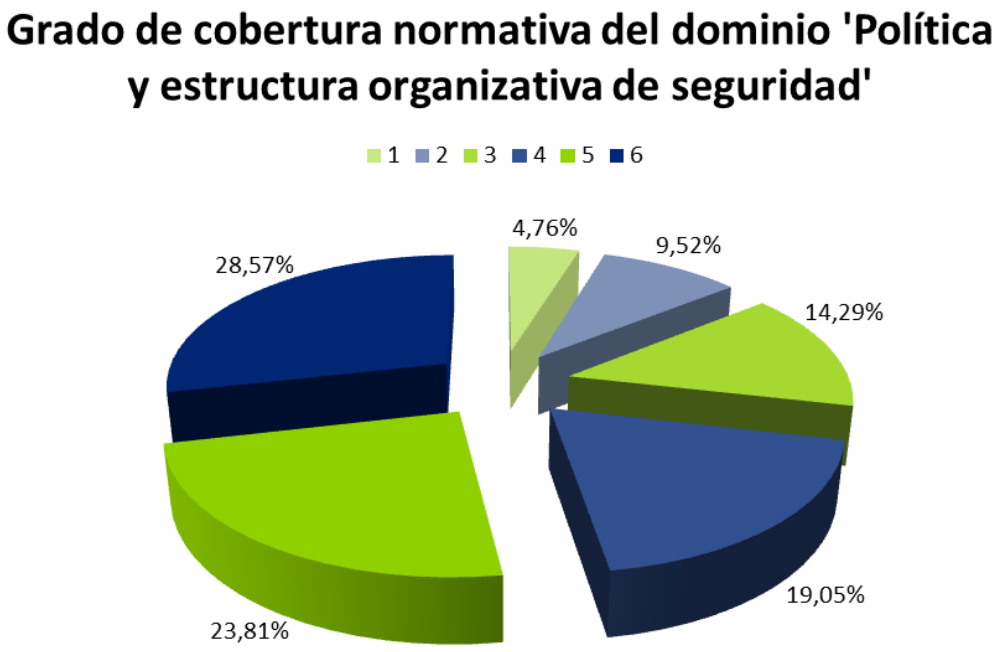

Ilustración 15 - Grado de cobertura

  - Diagrama del nivel de cumplimiento: grado de cumplimiento en cuanto a diseño, implementación y eficacia operativa de cada actividad de control, agrupadas por subdominio.

    Tomando como base el dominio empleado anteriormente, se adjunta el diagrama simulado del nivel de cumplimiento agrupado por subdominio,

considerando datos ficticios. Los diferentes subdominios han sido clasificados en función de su grado de cumplimiento:

- Diseño: el subdominio se encuentra planteado de tal forma que mitiga el riesgo asociado. Por ejemplo, un proceso de baja de usuarios ha sido diseñado de tal forma que imposibilita o dificulta el acceso de usuarios suprimidos a los sistemas de información en un período de 2 días laborables.

- Implementación: el subdominio correctamente diseñado es ejecutado y llevado a cabo, de acuerdo a sus especificaciones, en un instante determinado del tiempo.

- Eficacia operativa: el subdominio opera de acuerdo a sus especificaciones a lo largo de un periodo, por lo que su riesgo asociado se encuentra mitigado a lo largo de dicho período.

  A continuación, se detalla el nivel de cumplimiento en cuanto a diseño, implementación y eficacia operativa de uno de los dominios del modelo de control, constituido por sus correspondiente subdominios:

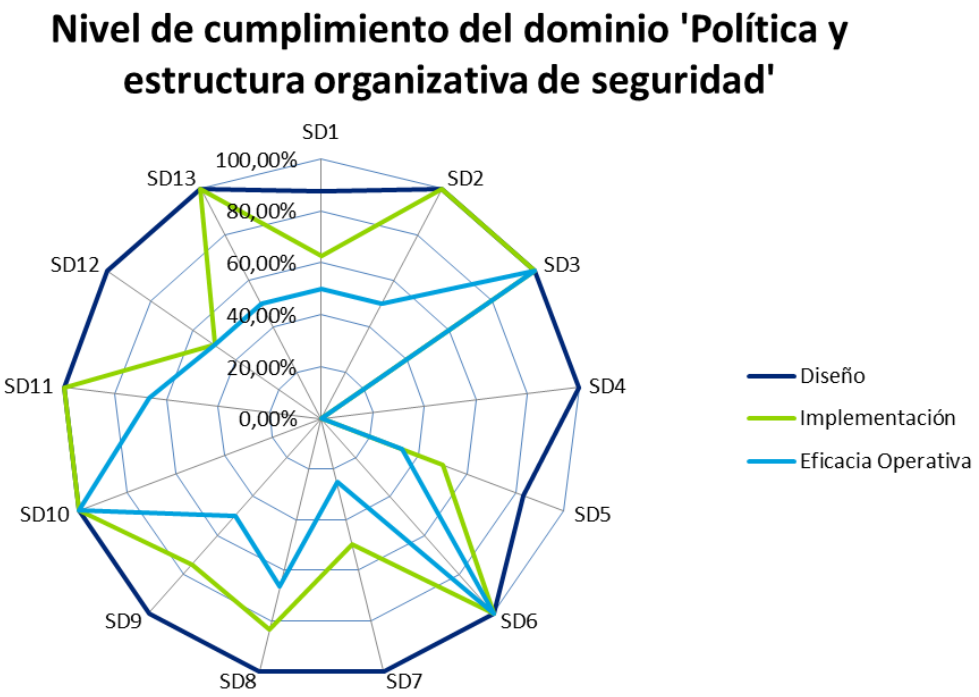

Ilustración 16 - Nivel de cumplimiento

Listado de subdominios:

SD1: Desarrollo de la Política de Seguridad.
SD2: Revisión y evaluación de la Política de Seguridad.
SD3: Estructura y funciones de los Comités de Seguridad.
SD4: Estructura y funciones del Grupo de coordinación.
SD5: Definición de funciones y responsabilidades de seguridad.

SD6: Personal especializado en seguridad.
SD7: Divulgación de la Información.
SD8: Formación y concienciación en seguridad.
SD9: Segregación de funciones de perfiles de seguridad y técnicos.
SD10: Segregación de funciones operacionales.
SD11: Identificación y clasificación de parámetros de riesgo de acceso.
SD12: Gestión de recursos por personal externo.
SD13: Riesgos asociados al logro de objetivos.

5. Caso de estudio

Se describe el proceso seguido en una sociedad en la cual se está realizando la implantación de un modelo de control.

Situación inicial

La compañía es una compañía del sector energético que, no siendo de las preminentes del sector, sí dispone de un volumen de negocio representativo.

El negocio de la entidad tiene una fuerte componente tecnológica, por lo que cuenta con un departamento de sistemas propio, que se dedica a la gestión de las actividades y tareas, estando la ejecución delegada en proveedores de servicios de tecnología.

La función de auditoría se encuentra formalizada y centralizada en el ámbito financiero, si bien no se dispone de una figura de auditoría interna en el área de sistemas de información.

El departamento de sistemas dispone de diferentes interlocutores que se encargan de centralizar la labor de cumplimiento normativo de las diferentes regulaciones aplicables.

Cumplimiento normativo

La labor de cumplimiento normativo es canalizada a través del área de auditoría interna, compuesta por cinco personas, que dispone de una planificación de los diferentes hitos del cumplimiento normativo (revisiones internas, externas, certificaciones, etc.).

Las legislaciones y normativas con las que la compañía debe cumplir son las siguientes:

- Auditoría de estados financieros, cuya periodicidad es anual.
- Revisión del cumplimiento del Título VIII del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, cuya periodicidad es cada dos años.
- Sistema de Control de la Información Financiera (SCIIF), cuya periodicidad es anual.

Adicionalmente, la compañía estaba en fase de determinar la idoneidad de certificarse en la ISO270001, es decir, la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI).

Asimismo, el área de Auditoría Interna realiza periódicamente revisiones específicas sobre áreas de negocio o procesos, como parte de los cuales se realizan requerimientos a sistemas de información.

Sistemas de información

El área de sistemas de información no realiza revisiones específicas sobre sus plataformas y no dispone de un modelo de control en el cual se formalicen los controles de los que dispone para la gestión de los sistemas de información.

Adicionalmente, tanto por parte de los auditores internos y externos se reporta regularmente la dificultad de obtener información del área de sistemas de información, la cual, a su vez, indica que está sujeta a revisiones continuas.

Enfoque propuesto

El objetivo del enfoque propuesto es reducir el esfuerzo asociado al cumplimiento normativo en el área de Sistemas de Información, así como optimizar la planificación existente y la colaboración entre Auditoría Interna y Sistemas de Información.

Para ello, la planificación que se ha realizado consta de los siguientes hitos:

1. Establecimiento del alcance normativo que la compañía desea abarcar.

2. Definición de un modelo de control integrado, que permita:
    a. Aunar en un único marco la totalidad de los requerimientos normativos necesarios para el cumplimiento de la entidad.
    b. Determinar la información necesaria a proporcionar por parte de Sistemas de Información incluyendo: fecha en la que se necesita la información, período que debe cubrir la misma, características de la información necesaria y posibles selecciones posteriores.
    c. Establecer los responsables dentro de Sistemas de Información de cada uno de los controles definidos, los cuales:
        i. Obtendrán la información definida en el modelo.
        ii. Serán los interlocutores para la resolución de dudas técnicas.
        iii. Analizarán las posibles recomendaciones propuestas y elaborarán planes de mejora.
    d. Establecer un coordinador en Sistemas de Información, cuyas funciones sean las indicadas a continuación:
        i. Interlocución con Auditoría Interna para el seguimiento del grado de avance.
        ii. Interlocución, junto con Auditoría Interna, con los revisores o auditores externos del ámbito de sistemas.
        iii. Coordinación de los responsables internos de Sistemas de Información.

3. Definición del programa de Auditorías, en base a:
    a. Las necesidades de Auditoría Interna.
    b. Las directrices de Sistemas de Información, en lo tocante a la disponibilidad de recursos y reiteración de las pruebas.
    c. Los requerimientos de cumplimiento que exigen cada una de las normativas en alcance, es decir, la periodicidad y alcance que marca cada normativa para evidenciar su cumplimiento.

4. Implantación de un repositorio documental, en el cual se definan las actividades de control que conforman el marco, la información necesaria, la planificación, etc. El repositorio documental debe constituir el canal a través del cual se produzca el intercambio de información entre los diferentes interlocutores.

5. Establecimiento de una función, dirigida por Auditoría Interna, con la colaboración de Sistemas de Información, para el establecimiento de un proceso de mejora continua sobre el modelo de control, con el objetivo de que anualmente se realicen las siguientes actividades:
    a. Revisión y adaptación del modelo de control, de acuerdo a cambios en el marco normativo de la entidad.
    b. Aprobación de los planes de acción que surjan con motivo de deficiencias o recomendaciones identificadas.
    c. Seguimiento cuatrimestral de los planes de acción aprobados.

Progreso del proyecto

Actualmente, se han finalizado 4 de las 5 fases del enfoque del proyecto, tal y como se describe a continuación:

1. La definición del alcance del marco normativo de la compañía se ha establecido considerando las legislaciones que la compañía debe cumplir, establecidas por Auditoría Interna, junto con la norma ISO270001, propuesta de Sistemas de Información para certificar sus procesos a final del ejercicio.

2. El modelo de control ha sido definido primeramente a través de la realización de una revisión general de controles en el ámbito de las tecnologías de la información.

   Este hito ha sido considerado imprescindible por parte del equipo con el objetivo de obtener un conocimiento del grado de madurez del cumplimiento normativo del departamento de Sistemas de Información, es decir de las políticas, procedimientos y procesos existentes. Asimismo, se ha realizado para tener en consideración y poner de manifiesto a la compañía las principales deficiencias de control existentes y poder anticipar a la compañía los puntos en los cuales se estima que no se podrá alcanzar el nivel de cumplimiento exigible.

   Se han identificado y definido las funciones consideradas necesarias en el área de Sistemas de Información. Esto es:
   - Los responsables de las actividades de control que se han definido como parte de marco de control.
   - La función de coordinador dentro del área, destinada a realizar una función de coordinación y seguimiento.

   Asimismo, se han realizado jornadas explicativas a dichos actores para comentar el proyecto, su planificación e implicaciones, así como las responsabilidades que

corresponden a cada uno de los responsables. Adicionalmente, se recibieron los comentarios en el área de Sistemas de Información, cuyas inquietudes se articularon en torno a:

- Planificación en la obtención de la información necesaria para cada una de las revisiones.
  Se indicó, por parte del equipo del proyecto, que se tendrían en cuenta, tanto los plazos de obtención de información, que no deberán ser en repetitivos en exceso, así como las necesidades normativas a considerar en el programa de auditorías, a través de las cuales se debe cubrir un ejercicio o período de tiempo concreto.
- Canalización de las dudas u observaciones con motivo de las revisiones, con el objeto de minimizar el impacto de las mismas en la operativa.
  Se indicó, por parte del equipo del proyecto, que la función de coordinador dentro del área de Sistemas de Información debería ser quien liderara las reuniones iniciales de las revisiones y filtrar aquellas dudas o cuestiones para las que no fuese necesaria la intervención de personal operativo del área.

3. El programa de auditorías necesarias para abordar el marco de cumplimiento anteriormente indicado se ha definido, con la colaboración de Auditoría Interna, considerando:
   - Las sinergias existentes entre las evidencias que se necesiten por parte de los auditores internos / externos para dar cumplimiento a los diferentes requerimientos normativos.
   - La planificación de los hitos de cumplimiento, tanto de las revisiones realizadas ad hoc por Auditoría Interna, como de las revisiones por parte de entidades externas.

4. Se ha implementado una herramienta de cumplimiento en la que se establezcan las responsabilidades de las actividades de control, se defina la información necesaria para cada una de ellas y se determinen los plazos en los que esta deba estar disponible.
   La implantación de la misma ha generado una reacción muy positiva entre los interlocutores, ya que ejerce la función de vehículo a través del cual se gestiona el cumplimiento, reduciendo el esfuerzo de los diferentes actores involucrados.

5. El establecimiento de una función de mejora continua del marco normativo no se establecido completamente, encontrándose en curso la definición de los indicadores aplicables, el modelo de reporting, las responsabilidades, etc. Se estima que en unas seis semanas se concluya la implementación de dicho modelo.

Lecciones aprendidas:

Las principales observaciones que se han realizado, de cara a futuras implantación de un modelo de control, pueden resumirse como sigue:

- Se debe hacer ver al departamento de sistemas que su función de cumplimiento normativo se verá optimizada en organización y tiempos, para contar con su colaboración en la iniciativa.
- El departamento de sistemas debe participar en la definición de las actividades de control que se hayan introducido en el marco debido a una regulación que ellos hayan solicitado, con el objetivo de minimizar su oposición en este punto.

Conclusión preliminar

En esta versión preliminar del modelo, en la cual se está abordando la fase más determinante, consistente en la implementación del proceso de mejora continua, se puede anticipar que la organización ha percibido de manera favorable la definición del modelo, puesto que entiende que establece un componente organizativo en el cumplimiento, así como que reduce el esfuerzo de la organización en adecuarse a las normativas.

Adicionalmente, la capacidad de convertir, a través de la herramienta implementada, el cumplimiento normativo en un proceso tangible, facilita la comprensión del mismo por parte de los actores involucrados, así como el entendimiento que éstos tienen del proceso.

A fecha de hoy, se considera, tanto por parte de los diferentes actores involucrados por la entidad como por parte del equipo, que ha sido un proyecto satisfactorio.

6. Planificación y presupuesto

Las fases e hitos de la consecución del proyecto han sido definidos en el siguiente plan de proyecto:

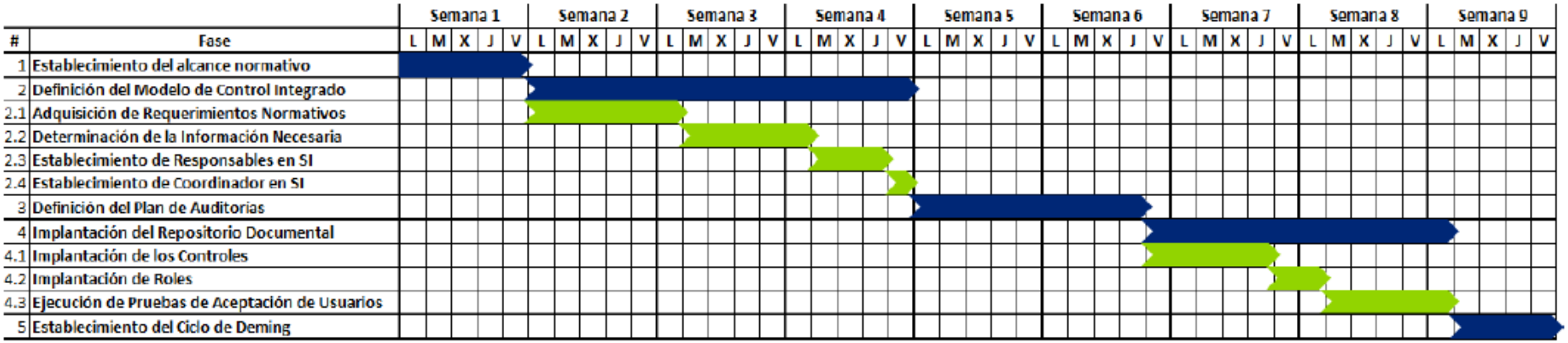

Ilustración 17 - Planificación

Para afrontar el Plan de Proyecto establecido se creará un grupo de trabajo conformado por un Director y un Gerente de proyecto con dedicación parcial (5% y 15% respectivamente), que compaginarán con otros proyectos así como un equipo de trabajo compuesto por un jefe de equipo (50% de dedicación) y un consultor con dedicación exclusiva. En base a dicho equipo, se establece un ratio medio por hora de aproximadamente 60 euros. Según la planificación del trabajo así como el esfuerzo dedicado por cada uno de sus miembros se estima que se dedicarán un total de 658 horas.

Es por ello que el coste total estimado del proyecto ascendería a **39.480 euros**.

7. Conclusiones

La presión e intensidad regulatorias a las que están sometidas las compañías en el entorno actual, junto con la coyuntura existente, que obliga a identificar eficiencias en todos los procesos, obliga a las compañías a estructurar y organizar su cumplimiento normativo, a fin de impactar lo menos posible en el *business as usual* de la organización.

La integración de los modelos de control representa una eficiencia en el proceso de cumplimento normativo, especialmente a aquellas compañías de tamaño mediano o grande, que están sometidas a una mayor presión regulatoria o legislativa.

La unificación de los modelos de control internos, a través del análisis de la identificación de las normativas de aplicación, junto con la definición de requerimientos únicos, permite llevar a cabo la integración de las actividades que conforman el cumplimiento normativo.

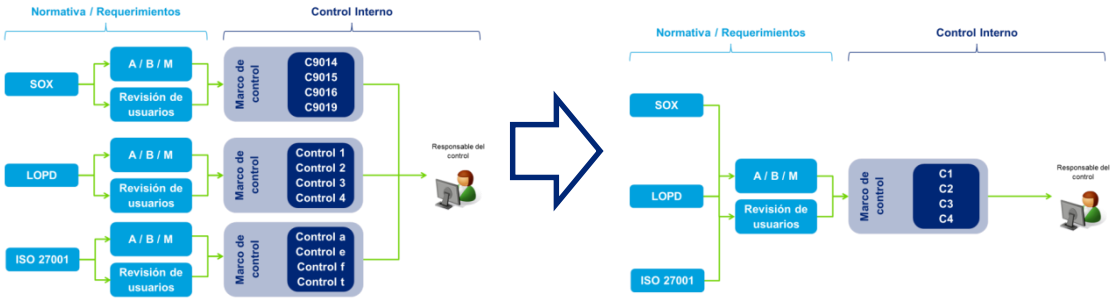

Ilustración 18 - Integración de modelos

Adicionalmente, la identificación de las responsabilidades dentro del proceso de cumplimiento normativo, que tiende a ser gestionado de forma descentralizada, permite a las compañías no sólo conseguir eficiencias en el proceso, sino también determinar unívocamente las responsabilidades, eliminando posibles duplicidades

Asimismo, la definición y formalización de las actividades de control que la compañía, especialmente el departamento de sistemas de información en el que impactan un gran número de las regulaciones, permite internamente a la compañía dotar de mayor visibilidad al proceso de cumplimiento normativo, concediéndole mayor visibilidad.

Finalmente, la capacidad de que un proceso sea medible a través de un conjunto de indicadores objetivos, permite la presentación del proceso a la alta dirección, así como una monitorización ágil del estado del mismo.

8. Líneas futuras

El cumplimiento normativo es un proceso que va ganando significancia paulatinamente en la operativa de las compañías, debido a, como ya se ha comentado, la creciente presión regulatoria. Ello hace necesario que el enfoque reactivo hacia el mismo no sea la manera más eficiente de abordarlo, sino que las entidades deben buscar formas de hacer más eficiente el proceso.

Se muestran en el siguiente gráfico los grados de madurez en los que se puede encontrar el cumplimiento normativo:

Ilustración 19 - Futuras líneas

Los enfoques reactivo y mixto ya han sido comentados a lo largo del documento, son aquellos en los cuales se encuentra la gran mayoría de entidades a día de hoy.

Enfoque preventivo

El enfoque preventivo es el enfoque propuesto en el presente documento, a través de la definición de un modelo de control integrado que incorpore todos los requerimientos de las diferentes normativas.

Asimismo, el modelo de control integrado se puede complementar a través de la implantación de un repositorio en el que se almacenen de manera centralizada las evidencias requeridas por las auditorías.

Auditoría continua

La auditoría continua es el siguiente nivel de madurez del cumplimiento normativo, vertebrado principalmente por dos aspectos:

- Herramientas de auditoría: implantación de herramientas de auditoría que periódicamente ejecuten las actividades de control. Estas herramientas facilitan enormemente a la compañía el cumplimiento con las normativas o legislaciones que les son de aplicación y reducen sustancialmente la participación de los operadores en la ejecución de las actividades de control.

  Por ejemplo, existen herramientas de código abierto que con la periodicidad especificada comprueban la configuración de un conjunto de servidores con respecto a las especificaciones de una guía de bastionado.

Ilustración 20 - Herramientas de auditoría

- Herramienta de cumplimiento normativo: las herramientas de cumplimiento normativo implementan el modelo de control integrado, contienen los inventarios de alcance, las actividades de control, definen las responsabilidades, establecen la planificación y contienen o referencias a las evidencias. Asimismo, alojan los planes de acción y permiten el establecimiento de indicadores a través de cuadros de mando.

  Dichas herramientas son accedidas por los diferentes actores que conforman el cumplimiento normativo:

  - Responsables de control: ejecutan y actualizan sus actividades de control, almacenando las evidencias en el repositorio.
  - Cumplimiento normativo: son responsables del mantenimiento del modelo de control integrado, tanto las normativas aplicables, inventarios de sistemas, actividades de control, cumplimiento de planificación, etc.

- Control interno: define, coordina y ejecuta el calendario de auditorías que revisan el cumplimiento normativo de la entidad. Asimismo, es quien realiza el reporte de resultados a la dirección.

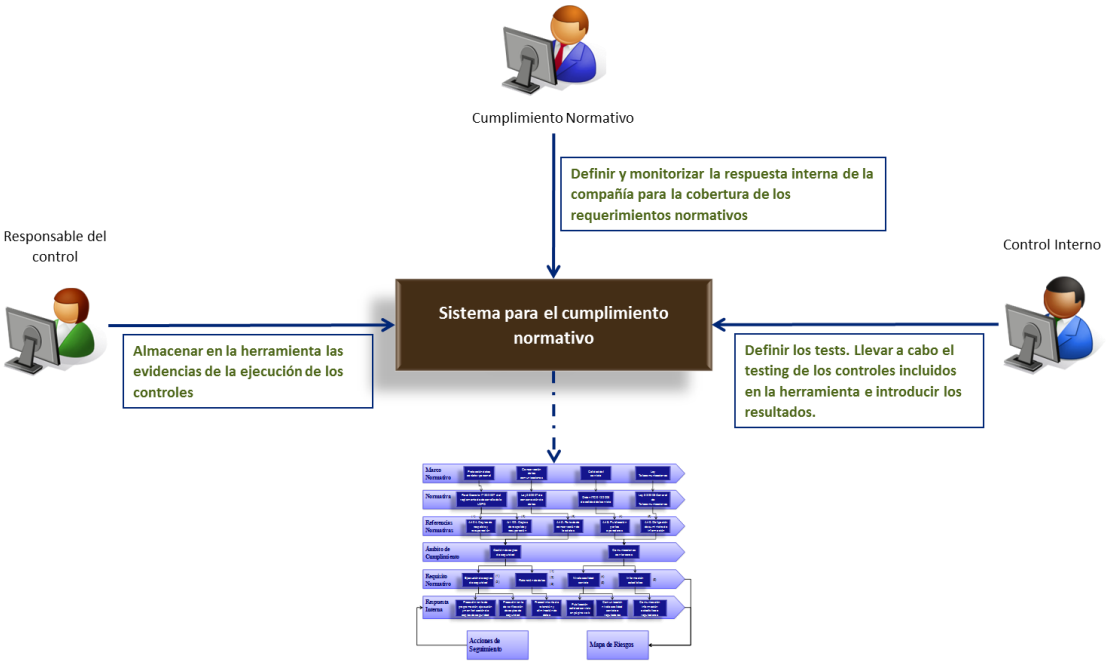

Ilustración 21 - Herramientas de cumplimiento

9. Agradecimientos

En este apartado sencillamente querría agradecer principalmente a Juanmi, Chema y Ángel, por sus opiniones, comentarios y sobre todo su paciencia durante el proyecto.

Asimismo, agradecer a mi compañero Luismi la dedicación empleada para que hayamos sacado adelante este último hito de la carrera.

Finalmente, lamentando ser tan escueto, entiendo que Galicia tiene algo que ver, agradezco a mis progenitores la ayuda y el apoyo constante a lo largo de estos años, difícilmente podré yo devolver la moneda.

10. Anexo I: Referencias

El presente apartado incluye un conjunto de documentación de referencia para diferentes aspectos mencionados a lo largo del documento. Asimismo, se han incluido apartados que incorporan una breve descripción, así como la referencia correspondiente, de las siguientes normativas, regulaciones o buenas prácticas:

- 10.1 ISO27002.
- 10.2 Cobit.
- 10.3 ITIL v3.
- 10.4 COSO.
- 9.6 LOPD.
- 9.7 PCI-DSS
- 9.8 SOX
- 9.9 SCIIF
- Ciclo de Deming

  http://asq.org/index.aspx

  http://www.quality-improvement-matters.com/

10.1. ISO27002

ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de Information technology - Security techniques - Code of practice for information security management.

El estándar establece unas "líneas y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información dentro de una organización". Los controles que figuran en la norma tienen por objeto atender las necesidades específicas identificadas por medio de una evaluación de riesgos formal.

Por otra parte, el la norma ISO/IEC 27002 también tiene por objeto proporcionar una guía para el desarrollo de "estándares en la organización para conseguir una eficaz gestión de las prácticas relativas a la gestión de la seguridad".

En 2013 ha sido publicada una nueva versión de la norma: ISO 27002:2013. Esta nueva versión ofrece una mayor granularidad respecto a sus antecesoras. Está compuesta por 113 controles subdivididos en 14 secciones:

- Estructura.
- Políticas de Seguridad.
- Organización de la seguridad de la información.
- Seguridad de recursos humanos.
- Gestión de activos.
- Control de acceso.
- Criptografía.
- Seguridad física y del entorno.
- Seguridad de las operaciones.
- Seguridad en la comunicación.
- Adquisición, desarrollo y mantenimiento de sistemas de la información.
- Relación con proveedores.
- Gestión de incidencias en la seguridad de la información.
- Aspectos de la seguridad de la información relacionada con la continuidad de negocio.
- Cumplimiento.

Fuente: http://www.27000.org/

10.2. Cobit

COBIT (en inglés Control Objectives for Information and related Technology), que significa Objetivos de Control para la información y Tecnologías relacionadas. Recoge un conjunto de buenas prácticas para el manejo de información que ha sido creado por la Asociación para la Auditoría y Control de Sistemas de Información ISACA (Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992. La última versión de COBIT se denomina COBIT 5, publicada en diciembre de 2012 y actualizada en junio de 2013.

El principal propósito de COBIT es investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control para las tecnologías de la información que sean autorizados, actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores.

Para conseguir dicho propósito COBIT se basa en 5 principios:

1. Satisfacción de las necesidades de los stakeholders
2. Cubrir los procesos de la organización de extremo a extremo (End-to-End)
3. La aplicación de un marco único e integrado
4. Implantación de un enfoque holístico
5. La separación del gobierno de la gestión de la organización

Fuente: http://www.isaca.org/

10.3. ITIL v3

ITIL (del inglés *Information Technology Infrastructure Library*), es un conjunto de conceptos y buenas prácticas para la del desarrollo, las operaciones y la gestión de servicios de tecnologías de la información. ITIL proporciona descripciones detalladas de un conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de tecnologías de la información. En junio de 2007 se publicó la última versión de ITIL conocida como ITIL v3.

ITIL v3 consolida el modelo de "ciclo de vida del servicio". Consta de 5 libros basados en el ciclo de vida del servicio:

1. Estrategia del Servicio.
2. Diseño del Servicio.
3. Transición del Servicio.
4. Operación del Servicio.
5. Mejora Continua del Servicio.

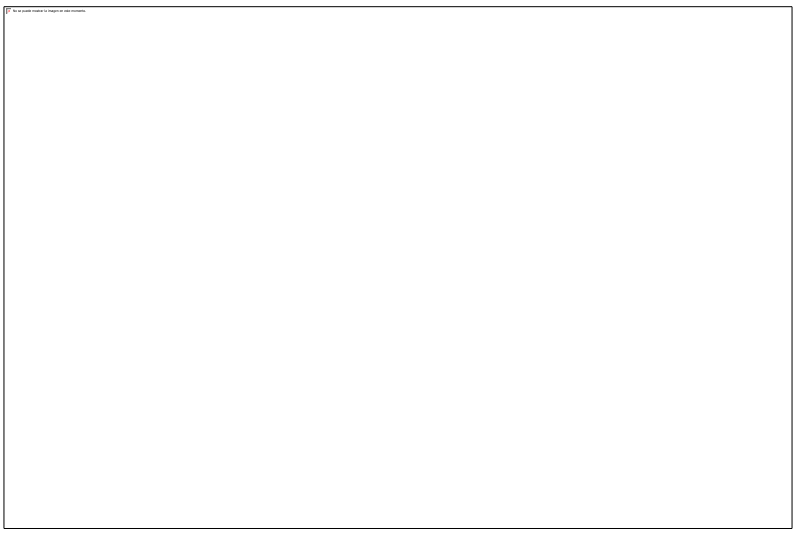

Ilustración 22 - ITIL

Fuente: http://www.best-management-practice.com/

10.4. COSO

El Marco Integrado de Control Interno COSO permite a las organizaciones desarrollar sistemas de control interno de una manera efectiva y eficaz que se adapten a negocios cambiantes y entornos operativos, mitigando los riesgos hasta niveles adecuados, y apoyando la toma de decisiones y el gobierno en la organización.

El diseño e implementación de un marco de un sistema de control interno puede ser un reto. Los nuevos y cambiantes modelos de negocio, el amplio uso de medios tecnológicos y la dependencia que surge con ellos, el aumento de requerimientos regulatorios, y otras necesidades necesitan de un sistema de control interno que se adapte ágilmente.

Un sistema de control interno efectivo requiere más que la adhesión de políticas y procedimientos, requiere el uso de buen juicio. Los comités ejecutivos usan el buen juicio para determinar cuan necesario es un control. El personal de gestión usan el buen juicio cada día para seleccionar, desarrollar, e implementar controles en la entidad. Los auditores internos utilizan el buen juicio para evaluar la eficacia operativa de los controles implementados.

El marco de control ofrece al comité ejecutivo y a la gestión:

- Los mecanismos para aplicar un marco de control independientemente de la entidad, industria, sector, estratificación, unidad operativa o función.
- Una solución basada en principios enfocada a proporcionar flexibilidad y buen juicio en el diseño, implementación y explotación de los controles.
- Los requerimientos para un sistema de control interno considerando como los componentes y procedimientos interactúan entre ellos.
- Los mecanismos para identificar y analizar riesgos, desarrollar y gestionar respuestas adecuadas hasta niveles aceptables, con un centrándose en gran medida en mecanismos anti fraude.
- La posibilidad de expandir el aplicativo de control interno más allá del reporte financiero.
- La posibilidad de eliminar controles inefectivos, redundantes o ineficientes que proporcionan poco valor a la reducción de riesgos en la consecución de los objetivos de la entidad.

Fuente: http://www.coso.org/

10.5. LOPD

La Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) es una Ley Orgánica española cuyo fundamental objetivo es la garantía y protección, en lo referente al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas. Especialmente de su honor, intimidad y privacidad.

Dicha Ley se encuentra desarrollada tanto en sus principios, como en las medidas de seguridad a aplicar en los sistemas de información mediante el Real Decreto 1720/2007 del 21 de Diciembre.

Principalmente tiene como objeto regular el tratamiento de los datos y ficheros de carácter personal, independientemente del soporte en el cual sean tratados así como los derechos de la ciudadanía sobre ellos y las obligaciones de aquellos que los crean o tratan.

Cuando un primero cede sus datos de carácter personal a segundo con una finalidad, se considera que existe tratamiento de datos por parte del segundo y por ende, debe cumplir con la regulación correspondiente. El primero puede ser un empleado, un proveedor, un cliente, un ciudadano, etc. Cualquier persona física, no jurídica.

La entidad en España que tiene responsabilidad y autoría para supervisar el cumplimiento es la Agencia Española de Protección de Datos. Toda Empresa o Administración Pública debe registrar los distintos tratamientos (por finalidad) que realiza sobre Datos de Carácter Personal.

Las principales medidas comunes aplicables tanto a ficheros automatizados como no automatizados para el cumplimiento de la Ley son las siguientes:

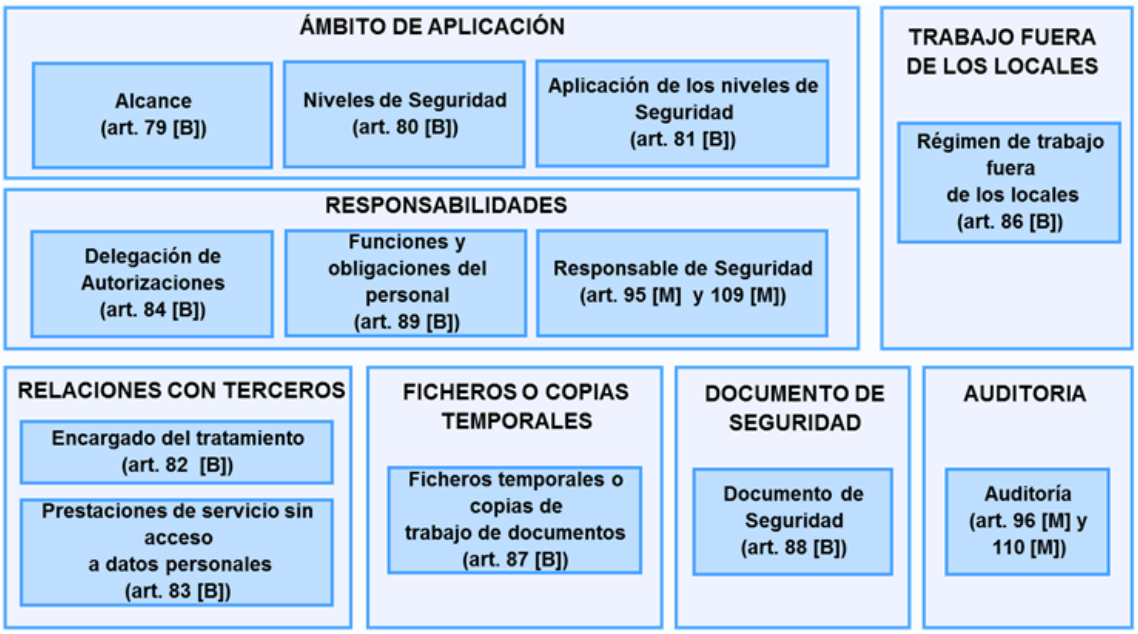

Ilustración 23 - Ámbitos LOPD

Fuente: http://www.agpd.es/

10.6. PCI-DSS

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial.

Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas. Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos.

A continuación, se muestra una descripción general de los 12 requisitos de las PCI DSS.

Normas de seguridad de datos de la PCI: descripción general de alto nivel

Desarrollar y mantener una red segura	1. Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta 2. No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
Proteger los datos del titular de la tarjeta	3. Proteja los datos del titular de la tarjeta que fueron almacenados 4. Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
Mantener un programa de administración de vulnerabilidad	5. Utilice y actualice con regularidad los programas o software antivirus 6. Desarrolle y mantenga sistemas y aplicaciones seguras
Implementar medidas sólidas de control de acceso	7. Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa 8. Asignar una ID exclusiva a cada persona que tenga acceso por computador 9. Restringir el acceso físico a los datos del titular de la tarjeta
Supervisar y evaluar las redes con regularidad	10. Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas 11. Pruebe con regularidad los sistemas y procesos de seguridad
Mantener una política de seguridad de información	12. Mantenga una política que aborde la seguridad de la información para todo el personal

Ilustración 24 - Dominios PCI - DSS

Fuente: https://www.pcisecuritystandards.org/

10.7. SCIIF

El SCIIF (Sistema de Control Interno sobre la Información Financiera) es una parte del control interno de la organización y se configura como el conjunto de procesos que el consejo de administración, el comité de auditoría, la alta dirección y el personal involucrado de la organización llevan a cabo para proporcionar un marco de seguridad razonable respecto a la fiabilidad de la información financiera que se publica en los mercados.

En 2010 la CNMV constituyó el Grupo de Trabajo de Control Interno sobre la información financiera (GTCI), con la finalidad de elaborar un conjunto de recomendaciones acerca del sistema de control interno sobre la información financiera

El resultado alcanzado por el GTCI son los siguientes:

1. Una propuesta de desarrollo normativo en materia de SCIIF.
2. Un marco de referencia que incluye un conjunto de principios generales y buenas prácticas de control interno sobre la información financiera para ayudar a las entidades cotizadas en el diseño, implantación, funcionamiento y supervisión de sus SCIIF que permita reforzar la fiabilidad de la información financiera.
3. Una guía para la preparación de la descripción del SCIIF.
4. Unas pautas de actuación para llevar a cabo la labor de supervisión de los comités de auditoría sobre el SCIIF.
5. Un glosario de términos.
6. Un modelo con los procedimientos para la revisión por el auditor externo.

El documento elaborado por el GTCI se dirige a la generalidad de las entidades cotizadas, con independencia de su tamaño, nivel de capitalización, naturaleza de los valores negociados o sector de actividad.

Fuente: http://www.cnmv.es/

10.8. SOX

La ley Sarbanes-Oxley (julio 2012) nace en Estados Unidos con el fin de monitorizar a las empresas que cotizan en bolsa, como reacción a los escándalos contables y de fraude corporativo que sacuden el mercado americano durante el periodo 2001-2002 (Enron, MCI Worldcom, etc.).

Tiene como objetivos disminuir el riesgo de fraude y controlar el riesgo de bancarrota de la empresa. Para cumplir con el primer objetivo, no se permite a la empresa emitir acciones por encima del valor que en verdad tiene la empresa. Para controlar el riesgo de bancarrota, se evita que la dirección del grupo o los auditores externos puedan aludir en su defensa el desconocimiento de los problemas que han dado origen a los problemas detectados.

Toda empresa que cotice en el NYSE (Bolsa de Valores de Nueva York) como a sus filiales y subsidiarias en otros países.

La sección 404 requiere que la empresa que cotiza cumpla:

- Asuma de manera explícita y al máximo nivel (CEO y CFO) su responsabilidad sobre el diseño, documentación, mantenimiento y evaluación periódica, del sistema de control interno que garantiza que toda la información financiera comunicada por ésta al mercado (Form 20-F) es fiable y está adecuadamente elaborada.

- Obtenga un informe donde su auditor externo emita una opinión independiente sobre (i) la evaluación realizada por el Grupo y (ii) la efectividad de su sistema de control interno de reporting financiero.

Fuentes: www.pcaobus.org y www.aicpa.org

11. Anexo II: Detalle a nivel de actividad de control del modelo de control integrado

En el presente anexo se adjunta, para el subdominio '***Análisis de riesgos"*** enmarcado dentro del dominio '***Política y estructura organizativa de seguridad***' el detalle de la integración llevada a cabo a nivel de actividad de control con cada una de las 8 normativas en alcance.

Como se puede observar, se ha asignado un identificador unívoco a cada una de las actividades de control (columna 'ID') en alcance así como un breve nombre descriptivo (columna 'Actividad de Control') que facilite la identificación de las mismas. Adicionalmente, se describe en detalle en qué consiste cada actividad de control (columna 'Narrativa') y el procedimiento para evaluar el nivel de cumplimiento de la misma, formulada a modo de pregunta (columna 'Cumplimiento'). Por último se indican los apartados, secciones o artículos correspondientes de las normativas que se encuentran cubiertos por cada una de las actividades de control.

					NORMATIVAS							
OBJETIVO DE CONTROL	**ACTIVIDAD DE CONTROL**	**NARRATIVA**	**CUMPLIMIENTO**	**ISO 27002**	**COBIT**	**ITIL**	**COSO**	**LOPD**	**PCI-DSS**	**SOX**	**SCIIF**
Política y estructura organizativa de seguridad											
4. Análisis de riesgos											
Identificación y clasificación de parámetros de riesgo de acceso											
4.0.1	*Identificación y clasificación de parámetros de riesgo de acceso*	*Metodología de análisis de riesgos*	Existencia de una metodología de análisis de riesgos basada en estándares reconocidos.	A la hora de permitir el acceso a cualquier activo de información del sistema, ya sea físico o lógico, por parte de personal externo (personal subcontratado, de empresas colaboradoras, etc.), ¿se ha realizado un análisis de los riesgos que	14.1.2	PO9.1, PO9.2, PO9.4, DS4.1, DS4.3	SS9.5, ST4.6, CSI5.6.3, SD4.4.5.2, SD4.5, SD4.5.5.2, SD4.5.5.4, SD8.1	10				

				supone dicho acceso?								
4.0.9	*Identificación y clasificación de parámetros de riesgo de acceso*	*Procedimiento para cumplir la metodología de riesgos*	Existencia de un procedimiento formal para aplicar la metodología de riesgos definida	¿Existe un procedimiento formal en el que se pueda aplicar la metodología de riesgos definida?	14.1.2	PO9.1, PO9.2, PO9.4, DS4.1, DS4.3	SS9.5, ST4.6, CSI5.6.3, SD4.4.5.2, SD4.5, SD4.5.5.2, SD4.5.5.4, SD8.1	10				
4.0.10	*Identificación y clasificación de parámetros de riesgo de acceso*	*Medidas de seguridad para mitigación de riesgos documentadas*	Documentación formal de las medidas de seguridad física y lógica, utilizadas para la mitigación de los riesgos identificados	¿Existe documentación formal de las medidas utilizadas en para mitigar los riesgos identificados?	14.1.2	PO9.1, PO9.2, PO9.4, DS4.1, DS4.3	SS9.5, ST4.6, CSI5.6.3, SD4.4.5.2, SD4.5, SD4.5.5.2, SD4.5.5.4, SD8.1	10				
Gestión de recursos por personal externo												

4.0.11	*Gestión de recursos por personal externo*	*Cláusulas de seguridad y confidencialidad*	Se establecerán cláusulas de seguridad y confidencialidad en los contratos de outsourcing	¿Hay establecidas cláusulas de seguridad y confidencialidad en los contratos de outsourcing?	6.2.2	PO6.2, DS5.4	SO4.5, SO4.5.5.1, SO4.5.5.2, SO4.5.5.3, SO4.5.5.4, SO4.5.5.5, SO4.5.5.6		83			
4.0.12	*Gestión de recursos por personal externo*	*Aprobación del propietario de los datos*	Se deberá obtener la aprobación por el propietario de los datos y del sistema antes de externalizar la gestión de los recursos	¿Existe una aprobación por parte del propietario de los datos y del sistema antes de externalizar la gestión de los recursos?	6.2.2	PO6.2, DS5.4	SO4.5, SO4.5.5.1, SO4.5.5.2, SO4.5.5.3, SO4.5.5.4, SO4.5.5.5, SO4.5.5.6					
Riesgos asociados al logro de objetivos												
SCIIF	*Riesgos asociados al logro de objetivos*		Deberán implantarse controles que respondan adecuadamente a los riesgos asociados al logro de los objetivos relacionados con la fiabilidad de la	¿Hay implatados controles dedicados a mitigar los riesgos que presenta la información financiera?								II.14

			información financiera, de tal forma que prevengan, detecten, mitiguen, compensen o corrijan su impacto potencial con la antelación necesaria									
SCIIF	*Riesgos asociados al logro de objetivos*		Deberán diseñarse y establecerse controles sobre los sistemas de información y comunicación con impacto en la información financiera y los cierres contables, de forma que garanticen, entre otros, la seguridad de acceso a datos y programas, el control sobre los cambios, la correcta operación de los mismos, su continuidad y la adecuada segrgación	¿Hay diseñados y establecidos controles sobre los SI y comunicación que impactan en la información financiera?								II.17

			de funciones									

Tabla 2 - Ejemplo de dominio integrado del modelo